

# DETECTING LARGE SIMPLE RATIONAL HECKE MODULES FOR $\Gamma_0(N)$ VIA CONGRUENCES

MICHAEL LIPNOWSKI AND GEORGE J. SCHAEFFER

**ABSTRACT.** We describe a novel method for bounding the dimension  $d$  of the largest simple Hecke submodule of  $S_2(\Gamma_0(N); \mathbb{Q})$  from below. Such bounds are of interest because of their relevance to the structure of  $J_0(N)$ , for instance.

In contrast with previous results of this kind, our bound does not rely on the equidistribution of Hecke eigenvalues. Instead, it is obtained via a Hecke-compatible congruence between the target space and a space of modular forms whose Hecke eigenvalues are easily controlled. For prime levels  $N \equiv 7 \pmod{8}$  our method yields an unconditional bound of  $d \geq \log_2 \log_2(\frac{N}{8})$ , improving the known bound of  $d \gg \sqrt{\log \log N}$  due to Murty–Sinha and Royer. We also discuss conditional bounds, the strongest of which is  $d \gg_\epsilon N^{1/2-\epsilon}$  over a large set of primes  $N$ , contingent on Soundararajan’s heuristics for the class number problem and Artin’s conjecture on primitive roots.

We also propose a number of Maeda-style conjectures based on our data, and we outline a possible congruence-based approach toward the conjectural Hecke simplicity of  $S_k(\mathrm{SL}_2(\mathbb{Z}); \mathbb{Q})$ .

## 1. INTRODUCTION

**1.1. Maeda’s conjecture and asymptotic simplicity.** It is natural to ask how spaces of modular forms decompose under the actions of their Hecke algebras.<sup>1</sup> Maeda’s conjecture attempts to answer this question in the level 1 case: It posits that for all even integers  $k \geq 4$  the  $\mathbb{Q}$ -vector space of weight  $k$  cusp forms for  $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$ , here denoted  $S_k(\Gamma(1); \mathbb{Q})$ , is a *simple* Hecke module. In fact, Maeda conjectured that this space is simple under the action of  $T_2$ .

Interesting arithmetic applications of Maeda’s conjecture have been noted by many authors: See Hida–Maeda [14], Conrey–Farmer [6], and Kohnen–Zagier [19] for a small sample. Computational evidence for Maeda’s conjecture has been given by

---

<sup>1</sup>Throughout this article, when  $V$  is a space of modular forms of level  $N$ , then by “the Hecke algebra of  $V$ ” we always mean the (commutative) subalgebra  $\mathbb{T}(V)$  of  $\mathrm{End}(V)$  generated by the Hecke operators  $T_n$  for  $n$  *relatively prime* to  $N$ . This is sometimes referred to as the *anemic* Hecke algebra. If  $V$  is clear from context we may denote its Hecke algebra simply by  $\mathbb{T}$ .

Buzzard [4], Farmer–James [10], and Ghitza–McAndrews [11], among others. At the time of writing, Maeda’s conjecture has been verified for weights  $k \leq 14000$ .

Another well-studied sequence of  $\mathbb{Q}$ -vector spaces of modular forms is

$$(*) \quad \{ S_2(\Gamma_0(N); \mathbb{Q}) : N \text{ prime} \}.$$

The Hecke module decompositions of the terms in this sequence have attracted interest because of established bijective correspondences between

- i. Simple Hecke submodules  $V' \subseteq S_2(\Gamma_0(N); \mathbb{Q})$  such that  $\dim_{\mathbb{Q}}(V') = d$ ;
- ii.  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -orbits  $\mathcal{O}$  of normalized cuspidal eigenforms in  $S_2(\Gamma_0(N); \overline{\mathbb{Q}})$  such that  $|\mathcal{O}| = d$ ; and
- iii. Simple isogeny factors  $A$  of  $J_0(N)$ , the Jacobian of the modular curve  $X_0(N)$ , such that  $\dim_{\mathbb{Q}}(A) = d$ .

In contrast with what Maeda predicts in the level 1 setting, the terms in the sequence  $(*)$  are *almost never* simple Hecke modules. The principal obstruction to simplicity in this case is the existence of the level  $N$  *Atkin–Lehner involution*  $w_N : f(\tau) \mapsto f(-\frac{1}{N\tau})$  on  $S_2(\Gamma_0(N); \mathbb{Q})$  [2]. Since the nebentypus is trivial,  $w_N$  commutes with the Hecke operators, so the  $\pm 1$ -eigenspaces of  $w_N$  are themselves Hecke submodules of  $S_2(\Gamma_0(N); \mathbb{Q})$  and we obtain a decomposition

$$S_2(\Gamma_0(N); \mathbb{Q}) = S_2(\Gamma_0(N); \mathbb{Q})^+ \oplus S_2(\Gamma_0(N); \mathbb{Q})^-$$

of *Hecke modules*. Both factors in this decomposition are nontrivial for  $N$  sufficiently large.<sup>2</sup> The difference  $\dim_{\mathbb{Q}} S_2(\Gamma_0(N); \mathbb{Q})^+ - \dim_{\mathbb{Q}} S_2(\Gamma_0(N); \mathbb{Q})^-$  can be expressed explicitly in terms of class numbers of imaginary quadratic fields, and well-known class number bounds then imply that this difference is  $\ll_{\epsilon} N^{1/2+\epsilon}$ . It follows that

$$\lim_{N \rightarrow \infty} \left( \frac{\dim_{\mathbb{Q}} S_2^+(\Gamma_0(N); \mathbb{Q})}{\dim_{\mathbb{Q}} S_2(\Gamma_0(N); \mathbb{Q})} \right) = \lim_{N \rightarrow \infty} \left( \frac{\dim_{\mathbb{Q}} S_2^-(\Gamma_0(N); \mathbb{Q})}{\dim_{\mathbb{Q}} S_2(\Gamma_0(N); \mathbb{Q})} \right) = \frac{1}{2}.$$

By way of illustration, we tabulate the dimensions of the Hecke-simple factors of  $S_2(\Gamma_0(N); \mathbb{Q})^{\pm}$  for prime levels  $N \in [10007, 10103]$  below (data over a broader range are given in Table 3 of §4.1):

---

<sup>2</sup>In fact, both factors in this decomposition are nontrivial as long as

$$N \neq 2, 3, 5, 7, 11, 13, 17, 19, 29, 31, 41, 47, 59, 71.$$

$N$	$S_2(\Gamma_0(N); \mathbb{Q})^+$	$S_2(\Gamma_0(N); \mathbb{Q})^-$	$N$	$S_2(\Gamma_0(N); \mathbb{Q})^+$	$S_2(\Gamma_0(N); \mathbb{Q})^-$
10007	[455]	[379]	10069	[432]	[406]
10009	[440]	[393]	10079	[486][1]	[353]
10037	[438]	[398]	10091	[458][1]	[382]
10039	[452]	[384]	10093	[430]	[410]
10061	[454]	[383][1]	10099	[443][1][1]	[396]
10067	[440]	[399]	10103	[446]	[394][2]

TABLE 1. Dimensions of simple Hecke submodules of  $S_2(\Gamma_0(N); \mathbb{Q})$ .

While  $S_2(\Gamma_0(N); \mathbb{Q})$  itself is almost never a simple Hecke module, data such as those in the table above suggest that the Atkin–Lehner eigenspaces  $S_2(\Gamma_0(N); \mathbb{Q})^\pm$  are *often* (but not always) simple. When they are *not* simple, it is due to the existence of small sporadic simple factors corresponding via modularity to elliptic curves and other low-dimensional abelian varieties with good reduction away from  $N$ . In Table 1, the 1-dimensional simple Hecke submodules correspond to elliptic curves of conductor equal to the level; the 2-dimensional Hecke submodule at level 10103 corresponds to an abelian surface of conductor  $10103^2$  having multiplication by an order in  $\text{Mat}_2 \mathbb{Q}(\sqrt{5})$ . In any case, one observes in the table that both  $S_2(\Gamma_0(N); \mathbb{Q})^+$  and  $S_2(\Gamma_0(N); \mathbb{Q})^-$  always contain a *large* simple Hecke submodule. Further computation seems to indicate that this “almost-simplicity” phenomenon continues as  $N$  grows.

In addition to the two sequences discussed so far, there are other sequences of  $\mathbb{Q}$ -vector spaces of modular forms whose terms seem to consistently admit large simple Hecke submodules. To ease notation, if  $V$  is a vector space over a field  $F$  and  $A$  is an  $F$ -subalgebra of  $\text{End}(V)$ , we set

$$\dim_{F,A}^* V = \max\{\dim_F V' : V' \text{ is an } F\text{-subspace of } V \text{ and a simple } A\text{-module}\}$$

For example, according to Table 1,  $\dim_{\mathbb{Q}, \mathbb{T}}^* S_2(\Gamma_0(10061); \mathbb{Q})^- = 383$ .

**Definition 1.1.** Let  $\{V_i\}_i$  be a sequence of vector spaces over a fixed field  $F$  and for each  $i$ , let  $A_i$  be an  $F$ -subalgebra of  $\text{End}(V_i)$ . We say that  $\{V_i\}_i$  is *asymptotically simple* (with respect to  $\{A_i\}_i$ ) if

$$\lim_{i \rightarrow \infty} \left( \frac{\dim_{F,A_i}^* V_i}{\dim_F V_i} \right) = 1.$$

Maeda’s conjecture implies that the sequence  $\{S_k(\Gamma(1); \mathbb{Q})\}_k$  is asymptotically simple (with respect to the terms’ Hecke algebras). We conjecture further that any sequence of spaces of modular forms with primitive nebentypen and with either the weight or the level tending to infinity is asymptotically Hecke-simple.

**Conjecture 1.2.** *Let  $\{(k_i, N_i, \chi_i)\}_i$  be a sequence of triples such that all  $k_i$  and  $N_i$  are positive integers and  $\chi_i : (\mathbb{Z}/N_i\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$  is primitive character satisfying  $\chi_i(-1) = (-1)^{k_i}$ . Let  $L = \mathbb{Q}(\{\chi_i\}_i)$ .*

- a. *If there is a fixed positive integer  $N$  and a fixed primitive  $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$  such that  $(N_i, \chi_i) = (N, \chi)$  for all  $i$ , and  $\{k_i\}_i$  is an increasing sequence; or*
- b. *If there is a fixed integer  $k \geq 2$  such that  $k_i = k$  for all  $i$ ,  $\{N_i\}_i$  is an increasing sequence, and  $L/\mathbb{Q}$  is a finite extension;*

*then the sequence  $\{S_{k_i}(N_i, \chi_i; L)\}_i$  of Hecke modules over  $L$  is asymptotically simple.*

We also conjecture that the Atkin–Lehner eigenspaces of  $S_k(\Gamma_0(N); \mathbb{Q})$  for fixed even weights  $k \geq 2$  and varying prime levels  $N$  are asymptotically simple.

**Conjecture 1.3.** *Let  $k$  be even and  $k \geq 2$ . The sequences*

$$\{S_k(\Gamma_0(N); \mathbb{Q})^+ : N \text{ prime}\} \quad \text{and} \quad \{S_k(\Gamma_0(N); \mathbb{Q})^- : N \text{ prime}\}$$

*of Hecke modules over  $\mathbb{Q}$  are asymptotically simple.*

While we avoid formal generalizations for brevity, the above conjectures can be adapted appropriately to cases where  $N$  is composite squarefree and/or the nebentypen are imprimitive, if one accounts for Hecke module decompositions induced by the Atkin–Lehner involutions.

We should add that Tsaknias [28] and Dieulefait–Tsaknias [7] have recently proposed conjectures that predict an exact count of the Galois orbits of normalized eigenforms in  $S_k(\Gamma_0(N); \overline{\mathbb{Q}})^{\text{new}}$  for *arbitrary* fixed  $N$  and  $k$  sufficiently large. Their prediction in the case of prime  $N$  is that there are *two* Galois orbits as  $k \rightarrow \infty$  (corresponding to the two Atkin–Lehner eigenspaces), which is certainly compatible with our Conjecture 1.3.

**1.2. Main results and methods.** Though we know no general method for constructing simple Hecke modules of the magnitude required to approach Conjectures 1.2 and 1.3, our main result, Theorem 1.4, certainly represents progress. It is perhaps especially encouraging in light of the conditional bounds given in Corollary 1.8.

Some notation: If  $k \geq 0$  and  $N \geq 1$  are integers,  $F$  is a field, and  $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow F^\times$  is a character, then by  $M_k(N, \chi; F)$  we mean the  $F$ -vector space of weight  $k$  *Katz modular forms* of level  $N$  and character  $\chi$  [17]. Its subspace of cusp forms is denoted  $S_k(N, \chi; F)$ .<sup>3</sup>

When  $R$  is a subring of  $F$  and  $N$  is invertible in  $R$ , then  $S_k(N, \chi; R)$  as defined in [17] coincides with the  $R$ -submodule of  $S_k(N, \chi; F)$  consisting of those forms whose  $q$ -expansions land in  $R[[q]]$ .

<sup>3</sup>When  $\text{char } F = 0$ , the space of Katz modular forms over  $F$  can be obtained from the corresponding space over  $\mathbb{Q}$  via extension of scalars. However, not all weight 1 Katz modular forms over  $\mathbb{F}_p$  can be obtained by mod- $p$  reduction of classical modular forms with coefficients in  $\mathbb{Z}$  [18, §4] [24, §5.1].

When  $\chi$  is trivial, we will usually replace the  $(N, \chi)$  in our notation for spaces of modular forms with the congruence subgroup  $\Gamma_0(N)$ . Finally, in what follows,  $\varepsilon_N$  will denote the quadratic character of conductor  $N$ .

**Theorem 1.4.** *Let  $N$  be squarefree with  $N \equiv 3 \pmod{4}$  so that  $\varepsilon_N(-1) = -1$ , and let  $p$  be a prime not dividing  $N$ . Set*

$$d_p(N) = \begin{cases} \dim_{\mathbb{Q}, \mathbb{T}}^* S_2(\Gamma_0(N); \mathbb{Q}) & \text{when } p = 2, \text{ and} \\ \dim_{\mathbb{Q}, \mathbb{T}}^* S_p(N, \varepsilon_N; \mathbb{Q}) & \text{when } p \text{ is odd.} \end{cases}$$

*Suppose that the class group of  $\mathbb{Q}(\sqrt{-N})$  has a cyclic quotient of order  $r$ , where  $r$  is not divisible by  $p$ , and let  $m$  be the order of  $p$  in  $(\mathbb{Z}/r\mathbb{Z})^\times / \{\pm 1\}$ . If  $m > 2$ , then  $d_p(N) \geq m$ .*

We prove Theorem 1.4 in §3. Roughly, the argument proceeds as follows: Let  $H_p$  denote the *mod  $p$  Hasse invariant*, which is an element of  $M_{p-1}(\Gamma(1); \mathbb{F}_p)$ . Multiplication by  $H_p$  yields an injective map

$$[H_p] : S_1(N, \tilde{\varepsilon}_N; \mathbb{F}_p) \rightarrow S_p(N, \tilde{\varepsilon}_N; \mathbb{F}_p) : f \mapsto H_p f$$

that is *Hecke-compatible* in the sense that  $[H_p] \circ T = T \circ [H_p]$  for all  $T \in \mathbb{T}$ . Note that when  $p = 2$ ,  $\tilde{\varepsilon}_N$  is the trivial character of level  $N$ , so  $[H_2] : S_1(\Gamma_0(N); \mathbb{F}_2) \rightarrow S_2(\Gamma_0(N); \mathbb{F}_2)$ .

Next, we consider the dihedral newforms in  $S_1(N, \varepsilon_N; \overline{\mathbb{Q}})$ . With notation as in the theorem, there is a dihedral newform with  $\zeta_r + \zeta_r^{-1}$  as a Hecke eigenvalue, and an explicit description of how the rational prime  $p$  factors in the extension  $\mathbb{Q}(\zeta_r + \zeta_r^{-1})/\mathbb{Q}$  allows us to produce a simple  $\mathbb{T}$ -submodule of  $S_1(N, \tilde{\varepsilon}_N; \mathbb{F}_p)$  having dimension at least  $m$ . By applying the map  $[H_p]$  we see that  $S_p(N, \tilde{\varepsilon}_N; \mathbb{F}_p)$  must also have a simple  $\mathbb{T}$ -submodule of dimension at least  $m$  and lifting back to characteristic zero yields the theorem.

In summary, we obtain the bound of Theorem 1.4 by combining the inequality

$$\dim_{\mathbb{F}_p, \mathbb{T}}^* S_1(N, \tilde{\varepsilon}_N; \mathbb{F}_p) \leq \dim_{\mathbb{F}_p, \mathbb{T}}^* S_p(N, \tilde{\varepsilon}_N; \mathbb{F}_p) \leq d_p(N)$$

with the control over  $\dim_{\mathbb{F}_p, \mathbb{T}}^* S_1(N, \tilde{\varepsilon}_N; \mathbb{F}_p)$  furnished by dihedral forms.<sup>4</sup>

**Remark 1.5.** As mentioned in the discussion of §1.1, simple Hecke-submodules of  $S_2(N; \mathbb{Q})$  of dimension  $d$  correspond bijectively with  $d$ -dimensional simple isogeny factors of the Jacobian  $J_0(N)$  of the modular curve  $X_0(N)$ . So as to avoid repetition later on, we emphasize here:

*Any lower bound on  $d_2(N)$  is also a lower bound on the dimension of the largest simple isogeny factor of  $J_0(N)$ .*

---

<sup>4</sup>The notation  $\dim^*$  is given before Definition 1.1.

That is, though Theorem 1.4 and Corollaries 1.6–1.8 are stated in the language of Hecke modules, they also provide information about the structure of  $J_0(N)$ .

**1.3. Unconditional bounds on  $d_2(N)$ .** Next we discuss how one can use Theorem 1.4 to obtain unconditional lower bounds on  $d_p(N)$ . Since these bounds are arguably most interesting when  $p = 2$ , we will concentrate on this case.

Serre showed in [26] that  $d_2(N)$  is unbounded. His argument, based on the equidistribution of the eigenvalues of  $T_\ell$  acting on  $S_2(N, \mathbb{C})$  for fixed prime  $\ell$  and increasing  $N$ , was made effective by Murty–Sinha [22] and Royer [23], establishing an asymptotic bound of  $d_2(N) \gg \sqrt{\log \log N}$  as  $N \rightarrow \infty$ .

Theorem 1.4 allows us to improve this bound for certain values of  $N$ :

**Corollary 1.6.** *With the notation and assumptions of Theorem 1.4, we have the lower bound  $d_2(N) \geq \log_2(r - 1)$ .*

*Proof.* The order of 2 in  $(\mathbb{Z}/r\mathbb{Z})^\times / \{\pm 1\}$  is easily seen to be at least  $\log_2(r - 1)$ . The result follows from Theorem 1.4.  $\square$

**Corollary 1.7.** *If, in addition to the assumptions of Theorem 1.4, we suppose that  $N$  is prime and  $N \equiv 7 \pmod{8}$ , then  $d_2(N) \geq \log_2 \log_2 \left(\frac{N}{8}\right)$ .*

*Proof.* Because  $N \equiv 7 \pmod{8}$ :

- a. The discriminant of  $K = \mathbb{Q}(\sqrt{-N})$  is  $-N$  and the ring of integers  $\mathbb{Z}_K$  is equal to  $\mathbb{Z} \left[ \frac{1 + \sqrt{-N}}{2} \right]$ .
- b. In light of (a.),  $N$  is the only prime ramified in  $K/\mathbb{Q}$ , so by genus theory, the class group of  $K$  has *odd order*.
- c. Since 2 is a quadratic residue modulo  $N$ , the (unramified) prime 2 splits in  $K/\mathbb{Q}$ , say  $2\mathbb{Z}_K = \mathfrak{p}\mathfrak{p}'$ .

Following an argument of Ellenberg–Venkatesh [8],  $\mathfrak{p}$  generates a large subgroup of the class group: Let  $r$  be the order of  $\mathfrak{p}$  in  $\text{Cl } K$ , so

$$\mathfrak{p}^r = (x + y\sqrt{-N}) \cdot \mathbb{Z}_K$$

for some  $x, y \in \frac{1}{2}\mathbb{Z}$ . Taking norms yields  $2^r = x^2 + Ny^2$ . Since  $r$  is odd by (b.) above,  $2^r \neq x^2$ , so we must have  $y \neq 0$ . Finally, because  $y^2 \geq \frac{1}{4}$  we have  $2^r \geq \frac{N}{4}$  and therefore  $r \geq \log_2\left(\frac{N}{4}\right)$ . The result now follows from the preceding corollary.  $\square$

**1.4. Conditional bounds on  $d_2(N)$ .** Recall the following well-known heuristics and conjectures due to Cohen–Lenstra (CL) [5], Soundararajan (S) [27], and Artin (A) [1] respectively:

- (CL) For an effective positive proportion of  $N \in [X, 2X]$ , the imaginary quadratic field  $\mathbb{Q}(\sqrt{-N})$  admits a cyclic quotient of odd order  $r \gg_\epsilon N^{1/2-\epsilon}$ .

- (S) There are positive constants  $a$  and  $b$ , not depending on  $r$ , such that the number  $n_r$  of imaginary quadratic fields with *prime* class number  $r$  satisfies  $ar < n_r \log r < br$
- (A) The element 2 generates  $(\mathbb{Z}/r\mathbb{Z})^\times$  for an effective positive density of primes  $r$ .<sup>5</sup>

Under various combinations of (CL), (S), and (A), Theorem 1.4 implies much stronger lower bounds for  $d_2(N)$  than the unconditional lower bound given in Corollary 1.7.

**Corollary 1.8.**      a. *Under (CL),*

$$d_2(N) \gg \log N$$

*for a positive proportion of squarefree integers  $N \in [X, 2X]$ .*<sup>6</sup>

b. *Under (S),*

$$d_2(N) \gg_\epsilon N^{1/4-\epsilon}$$

*for  $N$  lying in a subset of the squarefree integers in  $[X, 2X]$  of size  $\gg_\epsilon X^{1-\epsilon}$ .*

c. *Under (S) + (A),*

$$d_2(N) \gg_\epsilon N^{1/2-\epsilon}$$

*for  $N$  lying in a subset of the squarefree integers in  $[X, 2X]$  of size  $\gg_\epsilon X^{1-\epsilon}$ .*

To put Corollary 1.8 into perspective, note that any lower bound on  $d_2(N)$  obtained via Theorem 1.4 can never exceed the class number of  $\mathbb{Q}(\sqrt{-N})$ . Since this class number is at least  $\gg_\epsilon N^{1/2-\epsilon}$  and at most  $\ll_\epsilon N^{1/2+\epsilon}$ , the conditional asymptotic bound in (c.) above would essentially be the optimal bound accessible to our congruence method.

## 2. CONSEQUENCES OF ASYMPTOTIC SIMPLICITY FOR THE STRUCTURE OF $J_0(N)$

We next describe an application of Conjecture 1.3 to the arithmetic of  $J_0(N)$ .

Brumer conjectured in [3] that the rank of  $J_0(N)(\mathbb{Q})$  should be asymptotic to

$$\dim_{\mathbb{Q}} S_2(\Gamma_0(N); \mathbb{Q})^+ \sim \frac{1}{2} \dim_{\mathbb{Q}} S_2(\Gamma_0(N); \mathbb{Q})$$

as  $N \rightarrow \infty$ . The  $L$ -function of  $J_0(N)$  factors as a product of  $L(f, s)$  as  $f$  varies over the weight 2 level  $N$  cuspidal eigenforms for  $\Gamma_0(N)$ . Brumer's conjecture is “minimalist” in the sense that if  $L(f, s)$  vanished at the central point to the smallest order

<sup>5</sup>Artin's primitive root conjecture was proven by Hooley conditional on the Generalized Riemann Hypothesis [15].

<sup>6</sup>Assuming (CL), our main Theorem implies that  $d_2(N)$  is at least half the order of 2 in  $(\mathbb{Z}/r\mathbb{Z})^\times$  for some integer  $r \gg_\epsilon N^{1/2-\epsilon}$ . This will typically have order of magnitude *much* larger than  $\log N$ . The lower bound for  $d_2(N)$  from the above item is extremely wasteful but easily stated.

allowed by the sign of its functional equation and we assume the Birch–Swinnerton-Dyer (BSD) Conjecture, then there would be an *exact formula*<sup>7</sup>

$$(1) \quad \text{rank } J_0(N)(\mathbb{Q}) = \dim_{\mathbb{Q}} S_2(\Gamma_0(N); \mathbb{Q})^+.$$

Assuming the data in Table 1 is representative, Conjecture 1.3 should imply (1) for many prime  $N$ . Significantly more data concerning the small sporadic simple Hecke-submodules of  $S_2(N; \mathbb{Q})$  appears in §4.1.

**Proposition 2.1** (Exact formula for the rank of  $J_0(N)$  for some  $N$ ). *Assume BSD for  $J_0(N)$  and the Riemann Hypotheses for modular forms of weight 2 and for Dirichlet characters. Suppose also that the Atkin–Lehner eigenspaces  $S_2(\Gamma_0(N); \mathbb{Q})^{\pm}$  are simple  $\mathbb{T}$ -modules. Then*

$$\text{rank } J_0(N)(\mathbb{Q}) = \dim S_2(\Gamma_0(N); \mathbb{Q})^+.$$

**Remark 2.2.** The simplicity of  $S_2(\Gamma_0(N); \mathbb{Q})^+$  and  $S_2(\Gamma_0(N); \mathbb{Q})^-$  for large  $N$  is only plausible if  $N$  is prime.

*Proof.*  $J_0(N)$  is isogenous to  $J_0(N)^+ \times J_0(N)^-$ , where  $J_0(N)_{\pm}$  is the abelian subvariety of  $J_0(N)$  on which the Atkin–Lehner involution acts as  $\pm 1$ . By our assumption of simplicity,

$$\mathbb{T}(S_2(\Gamma_0(N); \mathbb{Q})) = K^+ \times K^-,$$

where  $K_{\pm} = \text{End}_{\mathbb{Q}}(S_2(\Gamma_0(N); \mathbb{Q})_{\pm})$  are fields. By BSD,  $J_0(N)^+(\mathbb{Q})$  contains a non-torsion point. The nonzero  $\mathbb{Q}$ -vector space  $J_0(N)^+(\mathbb{Q}) \otimes \mathbb{Q}$  is in fact a nonzero  $K^+$ -vector space. Thus,

$$\text{rank } J_0(N)^+ = \text{nonzero multiple of } [\dim_{\mathbb{Q}} K^+ = \dim_{\mathbb{Q}} S_2(\Gamma_0(N); \mathbb{Q})^+].$$

But if we had  $\text{rank } J_0(N)^+ \geq 2 \dim_{\mathbb{Q}} S_2(\Gamma_0(N); \mathbb{Q})^+$ , then we would have

$$(2) \quad \liminf_{N \rightarrow \infty} \frac{\text{rank } J_0(N)}{\dim_{\mathbb{Q}} S_2(\Gamma_0(N); \mathbb{Q})} \geq \liminf_{N \rightarrow \infty} \frac{\text{rank } J_0(N)^+}{\dim_{\mathbb{Q}} S_2(\Gamma_0(N); \mathbb{Q})} \geq 1.$$

However, (2) contradicts the result of Iwaniec–Luo–Sarnak [16] that

$$(3) \quad \frac{\text{rank } J_0(N)}{\dim_{\mathbb{Q}} S_2(\Gamma_0(N); \mathbb{Q})} \leq c + o(1)$$

for some explicit constant  $c < 1$ . Therefore, we must have

$$(4) \quad \text{rank } J_0(N)^+ = \dim_{\mathbb{Q}} S_2(\Gamma_0(N); \mathbb{Q})^+.$$

Now, since  $J_0(N)^-(\mathbb{Q}) \otimes \mathbb{Q}$  is a vector space over  $K^-$ , its rank must be a multiple of  $\dim_{\mathbb{Q}} S_2(\Gamma_0(N); \mathbb{Q})^-$ . If it is a nonzero multiple, then one would have

$$(5) \quad \text{rank } J_0(N)^-(\mathbb{Q}) \geq \dim_{\mathbb{Q}} S_2(\Gamma_0(N); \mathbb{Q})^-.$$

---

<sup>7</sup>The functional equation for  $L(f, s)$  has sign  $-\epsilon$  where  $\epsilon$  is the Atkin–Lehner eigenvalue of  $f$ . This is the reason  $S_2(\Gamma_0(N); \mathbb{Q})^+$  appears in formula (1) instead of  $S_2(\Gamma_0(N); \mathbb{Q})^-$ .



Combining (5) with what we know from (4) gives

$$\begin{aligned}
 \text{rank } J_0(N) &= \text{rank } J_0(N)^+ + \text{rank } J_0(N)^- \\
 &= \dim_{\mathbb{Q}} S_2(\Gamma_0(N); \mathbb{Q})^+ + \text{rank } J_0(N)^- \\
 &\geq \dim_{\mathbb{Q}} S_2(\Gamma_0(N); \mathbb{Q})^+ + \dim_{\mathbb{Q}} S_2(\Gamma_0(N); \mathbb{Q})^- \\
 &= \dim_{\mathbb{Q}} S_2(\Gamma_0(N); \mathbb{Q}),
 \end{aligned}$$

again contradicting the result of Iwaniec–Luo–Sarnak. Therefore, (5) is false and

$$(6) \quad \text{rank } J_0(N)^- = 0.$$

Combining (4) and (6) gives

$$\text{rank } J_0(N) = \text{rank } J_0(N)^+ + \text{rank } J_0(N)^- = \dim_{\mathbb{Q}} S_2(\Gamma_0(N); \mathbb{Q})^+.$$

□

**Example 2.3.** Referring back to Table 1 from the introduction, if the rate of convergence in the  $o(1)$  term from (3) were sufficiently fast, Proposition 2.1 would imply that  $J_0(10007)$  has rank 379.

### 3. DETECTING SIMPLE RATIONAL HECKE SUBMODULES VIA CONGRUENCES WITH WEIGHT 1 MODULAR FORMS

This section is devoted to the proof of our main result.

*Proof of Theorem 1.4.* Let us recall the set-up:

- We have a squarefree positive integer  $N \equiv 3 \pmod{4}$  and a prime  $p \nmid N$ ;
- We assume that the class number of  $K = \mathbb{Q}(\sqrt{-N})$  has a cyclic quotient  $C$  of order  $r$  with  $p \nmid r$ ;
- We denote by  $m$  the order of  $p$  in  $(\mathbb{Z}/r\mathbb{Z})^\times / \{\pm 1\}$ , and we assume that  $m > 2$ .

To ease notation, set

$$V_p(N; R) = \begin{cases} S_2(\Gamma_0(N); R) & \text{if } p = 2, \text{ and} \\ S_p(N, \varepsilon_N; R) & \text{if } p \text{ is odd.} \end{cases}$$

Our goal is to prove that  $V_p(N; \mathbb{Q})$  contains a simple Hecke submodule of dimension at least  $m$ .

Since the characteristic polynomial of  $T_n$  acting on  $V_p(N; \mathbb{Q})$  and the characteristic polynomial of  $T_n$  acting on  $V_p(N; \mathbb{Z}_p)$  are identical and monic with coefficients in  $\mathbb{Z}$ , it is enough to show that there is a prime  $\ell_0$  such that characteristic polynomial of  $T_{\ell_0}$  acting on  $V_p(N; \mathbb{Z}_p)$  has an irreducible factor of degree  $\geq m$ .

Let  $\zeta_r$  be a fixed primitive  $r$ th root of unity in  $\overline{\mathbb{Q}}$ , and let  $\chi$  be the composition

$$\chi : \text{Cl } K \twoheadrightarrow C \xrightarrow{g \mapsto \zeta_r} \overline{\mathbb{Q}}^\times,$$

where  $g$  is a generator of  $C$ . By class field theory,  $\chi$  is associated with an everywhere-unramified character of  $\text{Gal}(\overline{\mathbb{Q}}/K)$  that we also denote by  $\chi$ .

Let  $I_\chi := \text{Ind}_K^\mathbb{Q} \chi$  be the 2-dimensional representation of  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  induced from  $\chi$ . The Galois representation  $I_\chi$  is associated with a weight 1 cusp form of level  $N$  and nebentypus  $\varepsilon_N$ . More precisely, there is a normalized cuspidal eigenform  $f_\chi \in S_1(N, \varepsilon_N; \overline{\mathbb{Z}})$  with  $q$ -expansion  $\sum_{n \geq 1} a_n q^n$  such that  $T_n f_\chi = a_n f_\chi$  for all  $n$  relatively prime to  $N$  and such that the characteristic polynomial of  $I_\chi(\text{Frob}_\ell)$  is  $X^2 - a_\ell X + \varepsilon_N(\ell)$  for all primes  $\ell \nmid N$ . Calculating the trace of  $I_\chi$  directly, we find that  $a_\ell = \chi(\text{Frob}_\ell) + \chi^{-1}(\text{Frob}_\ell)$  whenever  $\ell \nmid N$ . By Chebotarev's density theorem, we may choose a prime  $\ell_0 \nmid Np$  such that  $a_{\ell_0} = \zeta_r + \zeta_r^{-1}$ .

Fix an embedding  $\iota : \overline{\mathbb{Q}} \rightarrow \overline{\mathbb{Q}}_p$ . The image of  $f_\chi$  under the induced embedding  $\iota : S_1(N, \varepsilon_N; \overline{\mathbb{Z}}) \rightarrow S_1(N, \varepsilon_N; \overline{\mathbb{Z}}_p)$ , denoted  $f_\chi^\iota$ , is an eigenform in  $S_1(N, \varepsilon_N; \overline{\mathbb{Z}}_p)$  satisfying  $T_n(f_\chi^\iota) = \iota(a_n) f_\chi^\iota$  whenever  $(n, Np) = 1$ .

Next we consider two maps that commute with the Hecke operators  $T_n$  for all  $(n, Np) = 1$ :

- The reduction map

$$S_1(N, \varepsilon_N; \overline{\mathbb{Z}}_p) \otimes \overline{\mathbb{F}}_p \xrightarrow{\text{red}} S_1(N, \varepsilon_N; \overline{\mathbb{F}}_p)$$

is injective,  $\overline{\mathbb{F}}_p$ -linear, and Hecke-compatible in the sense that

$$\text{red}(T_n(h \otimes 1)) = T_n(\text{red}(h \otimes 1)) \text{ for all } h \in S_1(N, \varepsilon_N; \overline{\mathbb{Z}}_p)$$

- Multiplication by the Hasse invariant  $H_p \in M_{p-1}(\Gamma(1); \overline{\mathbb{F}}_p)$  yields an injective, Hecke-compatible map

$$[H_p] : S_1(N, \varepsilon_N; \overline{\mathbb{F}}_p) \rightarrow V_p(N; \overline{\mathbb{F}}_p) : f \mapsto H_p f$$

It follows that  $f = [H_p](\text{red}(f_\chi^\iota \otimes 1)) \in V_p(N; \overline{\mathbb{F}}_p)$  is nonzero and satisfies  $T_n(f) = \overline{\iota(a_n)} f$  for all  $n$  with  $(n, Np) = 1$ , the overline indicating reduction  $\overline{\mathbb{Z}}_p \rightarrow \overline{\mathbb{F}}_p$ . In particular,

$$(7) \quad T_{\ell_0} f = \lambda f, \quad \text{where } \lambda = \overline{\iota(\zeta_r) + \iota(\zeta_r^{-1})}.$$

Let  $\mathfrak{m}$  denote the maximal ideal of the Hecke algebra  $\mathbb{T}_{p, \overline{\mathbb{F}}_p}$  associated with the eigenvalue system  $\{\overline{\iota(a_n)}\}_{n, (n, Np)=1}$ . The Galois representation  $\bar{\rho}$  associated with  $\mathfrak{m}$  equals  $\overline{\iota I_\chi}$ , i.e., the composition of  $I_\chi$  with the ring homomorphism  $\bar{\iota} : \overline{\mathbb{Z}} \rightarrow \overline{\mathbb{F}}_p$ .

- Because  $r > 2$ ,  $\bar{\rho}$  is absolutely irreducible; indeed, its image is a nonabelian dihedral group acting in “the usual way” on a 2-dimension  $\overline{\mathbb{F}}_p$ -vector space.
- $\bar{\rho}$  is not induced from  $K_0 = \mathbb{Q}(\sqrt{-1})$  or  $\mathbb{Q}(\sqrt{-3})$ : To verify this, let  $\bar{\tau} = \text{Ind}_{K_0}^\mathbb{Q}(\chi_0)$  for some 1-dimensional representation  $\chi_0 : G_{K_0} \rightarrow \overline{\mathbb{F}}_p^\times$ . The fields  $K_0$  and  $\mathbb{Q}(\sqrt{-N})$  are linearly disjoint because  $N \neq 1, 3$ . By Chebotarev, we can find a rational prime  $v$  which is unramified for  $\bar{\rho}$ ,  $K_0$ , and  $\mathbb{Q}(\sqrt{-N})$ , and

for which (a.)  $\text{Frob}_v$  is the nontrivial element of  $\text{Gal}(K_0/\mathbb{Q})$  and (b.)  $\text{Frob}_v$  is the trivial element of  $\text{Gal}(\mathbb{Q}(\sqrt{-N})/\mathbb{Q})$ . By (b.),  $\bar{\rho}(\text{Frob}_v)$  is a scalar matrix. On the other hand,  $\bar{\tau}(\text{Frob}_v)$  is a non-scalar matrix by (a.). Therefore,  $\bar{\rho}$  cannot be isomorphic to  $\bar{\tau}$ .

By [18, Proposition 4.2],  $\mathfrak{m}$  is the image of a maximal ideal  $\tilde{\mathfrak{m}}$  for  $\mathbb{T}(V_p(N; \bar{\mathbb{Z}}_p))$  and the reduction map

$$V_p(N; \bar{\mathbb{Z}}_p)_{\tilde{\mathfrak{m}}} \otimes \bar{\mathbb{F}}_p \twoheadrightarrow V_p(N; \bar{\mathbb{F}}_p)_{\mathfrak{m}}$$

is surjective and Hecke-compatible. Therefore, for all  $\ell \nmid Np$ , the element  $\overline{\iota(a_\ell)} \in \bar{\mathbb{F}}_p$  is a root of the characteristic polynomial of  $T_\ell$  acting on  $V_p(N; \mathbb{Z}_p) \otimes \mathbb{F}_p$ , which is identical to the characteristic polynomial of  $T_\ell$  acting on  $V_p(N; \bar{\mathbb{Z}}_p) \otimes \bar{\mathbb{F}}_p$ .

Finally, the element  $\lambda \in \bar{\mathbb{F}}_p$  defined earlier in (7) generates an extension of  $\mathbb{F}_p$  having degree equal to the order of  $\text{Frob}_p \in \text{Gal}(\mathbb{Q}(\zeta_r + \zeta_r^{-1})/\mathbb{Q})$  (note that  $p$  is unramified since  $p \nmid r$ ). We have  $\text{Frob}_p = p$  under the identification

$$\text{Gal}(\mathbb{Q}(\zeta_r + \zeta_r^{-1})/\mathbb{Q}) = (\mathbb{Z}/r\mathbb{Z})^\times / \{\pm 1\},$$

so we may deduce that  $[\mathbb{F}_p(\lambda) : \mathbb{F}_p] = m$ , where  $m$  is the order of  $p$  in  $(\mathbb{Z}/r\mathbb{Z})^\times / \{\pm 1\}$ .

It follows that the characteristic polynomial of  $T_{\ell_0}$  acting on  $V_p(N; \mathbb{Z}_p) \otimes \mathbb{F}_p$  has an irreducible factor of degree  $m$ . Since the characteristic polynomial of  $T_{\ell_0}$  acting on  $V_p(N; \mathbb{Z}_p) \otimes \mathbb{F}_p$  is just the mod- $p$  reduction of the characteristic polynomial of  $T_{\ell_0}$  acting on  $V_p(N; \mathbb{Z}_p)$ , this latter polynomial must have an irreducible factor of degree  $\geq m$ , as desired.  $\square$

**Example 3.1.** Let  $N = 719$  (this is prime). The field  $\mathbb{Q}(\sqrt{-719})$  has class number 31, and of course, 2 has order 5 modulo 31.

The space  $S_1(719, \varepsilon; \mathbb{Q})$  is 15-dimensional and Hecke-simple. The characteristic polynomial of  $T_2$  acting on this space is irreducible over  $\mathbb{Q}$ , and it factors as

$$(8) \quad (X^5 + X^2 + 1)(X^5 + X^3 + 1)(X^5 + X^4 + X^3 + X^2 + 1)$$

over  $\mathbb{F}_2$ . Our method now yields the inequality

$$\dim_{\mathbb{F}_2, \mathbb{T}}^* S_2(\Gamma_0(719); \mathbb{F}_2) \geq \dim_{\mathbb{F}_2, \mathbb{T}}^* S_1(N, \varepsilon; \mathbb{F}_2) \geq 5,$$

and, by lifting to characteristic zero, we obtain  $d_2(719) = \dim^* S_2(\Gamma_0(719); \mathbb{Q}) \geq 5$ .

The characteristic polynomial of  $T_2$  acting on  $S_2(\Gamma_0(719); \mathbb{Q})$  factors as

$$(9) \quad (X^5 + 2X^4 - 4X^3 - 9X^2 - 2X + 1) \\ (X^{10} - 11X^8 + 2X^7 + 39X^6 - 12X^5 - 52X^4 + 16X^3 + 24X^2 - 5X - 1) \cdot P,$$

where  $\deg P = 45$ .

Note that the first factors in (8) and (9) are congruent modulo 2. That is, in this particular case, the method of Theorem 1.4 detects a simple rational Hecke submodule of dimension exactly equal to the lower bound  $m$ .

The other two factors in (8) divide the reduction of  $P$  modulo 2. A dimension argument shows that  $\ker P(T_2) = S_2(\Gamma_0(719); \mathbb{Q})^+$ . Thus, of the three factors in (8), the first comes from  $S_2(\Gamma_0(719); \mathbb{Q})^-$  while the second and third come from  $S_2(\Gamma_0(719); \mathbb{Q})^+$ .

**Example 3.2.** One advantage of our method is that it allows us to derive concrete lower bounds on  $d_2(N)$  without having to compute  $S_2(\Gamma_0(N); \mathbb{Q})$  directly. Below, we give the bounds obtained by Theorem 1.4 for some relatively high levels:

$N$	$\text{Cl } \mathbb{Q}(\sqrt{-N})$	$r$	$m$
81799	$C_{127}$	127	7
81839	$C_{377}$	377	42
81847	$C_{183}$	183	60
81883	$C_{35}$	35	12
81899	$C_{101}$	101	50

TABLE 2. Bounds on  $d_2(N)$  for large  $N$ .

Above,  $C_j$  is a cyclic group of order  $j$ ,  $r$  is the order of the largest cyclic quotient (all class groups were cyclic in this range), and  $m$  is the order of 2 in  $(\mathbb{Z}/r\mathbb{Z})^\times / \{\pm 1\}$ . By Theorem 1.4,  $d_2(N) \geq m$ . This allows us to conclude, for example, that the 6820-dimensional space  $S_2(\Gamma_0(81839); \mathbb{Q})$  admits a simple Hecke submodule of dimension  $\geq 42$ .

**Remark 3.3.** Suppose  $v = 2^p - 1$  is a Mersenne prime. Assuming Soundararajan's Conjecture [27, (C1)], there will exist some  $N$  for which  $\mathbb{Q}(\sqrt{-N})$  has class number  $v$ . This hypothetical integer  $N$  would have size of magnitude roughly  $2^{2p}$ , up to factors that are polynomial in  $p$ . On the other hand, the order of 2 in  $(\mathbb{Z}/v\mathbb{Z})^\times / \{\pm 1\}$  equals  $p$ , which has size roughly  $\frac{1}{2} \log N$ .

In the range of the example above, the unconditional bound of Corollary 1.7 is  $d_2(N) \geq \lceil \log_2 \log_2 \left( \frac{N}{8} \right) \rceil = 4$ , and this bound applies when  $N \equiv 7 \pmod{8}$ , as in the first three rows of Table 2. The  $m$  of the first row is so small because the class number happens to be a Mersenne prime.

#### 4. ALMOST-SIMPLICITY OF $S_2(\Gamma_0(N); \mathbb{Q})$

**4.1. Small rational Hecke modules for  $\Gamma_0(N)$ .** If  $R$  is a ring and  $f \in R[X]$ , let  $\deg_R^*(f)$  denote the largest degree of an irreducible factor of  $f$  (in  $R[X]$ ).

Let  $\Phi_{N,\ell}^\pm(X)$  denote the characteristic polynomial of  $T_\ell$  acting on  $S_2(\Gamma_0(N); \mathbb{Q})^\pm$  and set

$$\begin{aligned} \delta_{N,\ell}^\pm &= \deg_{\mathbb{Q}} \Phi_{N,\ell}^\pm - \deg_{\mathbb{Q}}^* \Phi_{N,\ell}^\pm \\ &= \dim_{\mathbb{Q}} S_2(\Gamma_0(N); \mathbb{Q})^\pm - \deg_{\mathbb{Q}}^* \Phi_{N,\ell}^\pm. \end{aligned}$$

$\delta_{N,\ell}^\pm$  captures the contribution to  $\dim_{\mathbb{Q}} S_2(\Gamma_0(N); \mathbb{Q})^\pm$  by *small* Hecke submodules. Conjecture 1.3 implies that for any  $\ell$  we have

$$\lim_{\substack{N \rightarrow \infty \\ N \text{ prime}}} \left( \frac{\delta_{N,\ell}^\pm}{\dim_{\mathbb{Q}} S_2(\Gamma_0(N); \mathbb{Q})^\pm} \right) = 0.$$

Empirically, much more appears true:  $\delta_{N,\ell}^\pm$  seems to behave like a *bounded quantity*. We computed  $\delta_{N,2}^\pm$  for the 1092 primes  $N \in [100, 9000]$ :

$\delta$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
freq. $\delta_{N,2}^+ = \delta$	860	87	85	19	14	11	4	5	2	3	0	0	1	0	0	1	0	0	0
freq. $\delta_{N,2}^- = \delta$	865	103	68	29	15	3	3	1	2	1	1	0	0	0	0	0	0	0	1

TABLE 3. Histogram for values of  $\delta_{N,2}^\pm$ .

For example,  $\delta_{N,2}^+ = 3$  for exactly 19 primes  $N \in [100, 9000]$ .

**4.2. Remarks on the size of  $\delta_{N,2}^\pm$ .** We will now try to give a plausible explanation for why  $\deg \delta_{N,2}^\pm$  is usually so small.

For every Hecke eigenform  $f \in S_2(N; \overline{\mathbb{Q}})$ , let  $I_f$  denote the kernel of the homomorphism  $\mathbb{T} \rightarrow \mathbb{C}$  induced by the action of the prime to  $N$  Hecke operators on  $f$ . Let  $\mathcal{O}$  denote the  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -orbit of  $f$ . Note that  $I_f$  depends only on  $\mathcal{O}$ . The Hecke algebra  $\mathbb{T}$  acts, by Picard functoriality, on the Jacobian  $J_0(N)$  of the modular curve  $X_0(N)$ . Let  $A_{\mathcal{O}} := J_0(N)/I_f$ , the so-called *optimal quotient* associated with  $f$ .

The abelian variety  $J_0(N)$  is isogenous to  $\prod_{\mathcal{O}} A_{\mathcal{O}}$ , where  $\mathcal{O}$  ranges over all the  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -orbits of normalized Hecke eigenforms in  $S_2(N; \overline{\mathbb{Q}})$ . The dimension of  $A_{\mathcal{O}}$  equals  $g_{\mathcal{O}} = \#\mathcal{O}$ . Furthermore,  $A_{\mathcal{O}}$  has  $\text{GL}_2$ -type for the field  $K_{\mathcal{O}}$  generated by the Hecke eigenvalues of one orbit representative, i.e.  $\deg(K_{\mathcal{O}}/\mathbb{Q}) = g_{\mathcal{O}}$  and the endomorphism algebra of  $A_{\mathcal{O}}$  equals  $\text{Mat}_2(K_{\mathcal{O}})$ . Because all Hecke eigenforms are new at prime level  $N$ , the abelian variety  $A_{\mathcal{O}}$  has conductor  $N^d$ . Furthermore,  $A_{\mathcal{O}}$  admits a canonical polarization whose degree  $d_{\mathcal{O}}$  is studied in [9].

Conversely, let  $A/\mathbb{Q}$  be an abelian variety of dimension  $d$  which is  $\text{GL}_2$ -type with respect to a totally real number field  $F/\mathbb{Q}$  of degree  $d$ . Suppose that  $A$  has conductor  $N^d$ . Thanks to Khare–Winterberger’s proof of Serre’s Conjecture and the current state of knowledge for modularity lifting theorems, every such  $A$  is isogenous to  $A_{\mathcal{O}}$  for some  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -orbit of Hecke eigenforms in  $S_2(N; \overline{\mathbb{Q}})$ .

Every abelian variety  $A_{\mathcal{O}}$  defines a rational point in  $\mathcal{A}_{g_{\mathcal{O}}, d_{\mathcal{O}}}(\mathbb{Q})$ , where  $\mathcal{A}_{g,d}$  denotes the moduli space of  $g$ -dimensional abelian varieties equipped with a polarization of degree  $d$ . These varieties tend to be general type for  $g$  and  $d$  large. For example, it is known that  $\mathcal{A}_{g,1}$  is general type for  $g > 6$  and is not for  $g < 6$ .

The Bombieri–Lang Conjectures suggest that  $V(\mathbb{Q})$  is “very thin” for  $V/\mathbb{Q}$  a variety of general type. As explained in the previous paragraph, every (non-repeated) irreducible factor of  $\delta_{N,2}^\pm$  of degree  $g$  gives rise to an element of  $\mathcal{A}_{g,d}(\mathbb{Q})$  for some

(controlled)  $d$ . This perhaps explains why the counts in Table 3 apparently “thin out” around  $\delta_{N,2}^{\pm} = 6$ .

## 5. DETECTING SIMPLE RATIONAL HECKE MODULES FOR $\Gamma(1)$ VIA CONGRUENCES

Though we have so far only been able to derive explicit bounds in the cases covered by Theorem 1.4, congruences between spaces of modular forms can potentially be used to study other families of Hecke modules. Interestingly, it may be possible to apply congruence methods toward the conjectural simplicity of spaces of level 1 cusp forms.

There is a well-known Hecke-compatible congruence between  $S_{p+1}(\Gamma(1), \mathbb{F}_p) = S_{p+1}(\mathrm{SL}_2(\mathbb{Z}); \mathbb{F}_p)$  and  $S_2(\Gamma_0(p); \mathbb{F}_p)$  [25, Théorème 11.b]. By an argument similar to the one made in the proof of our main theorem, this congruence implies

$$(10) \quad \dim_{\mathbb{Q}, \mathbb{T}}^* S_{p+1}(\Gamma(1); \mathbb{Q}) \geq \dim_{\mathbb{F}_p, \mathbb{T}}^* S_2(\Gamma_0(p); \mathbb{F}_p).$$

Let  $D_p$  be the common dimension of  $S_{p+1}(\Gamma(1))$  and  $S_2(\Gamma_0(p))$  over both  $\mathbb{Q}$  and  $\mathbb{F}_p$ , and let

$$\alpha_p = \frac{1}{D_p} \dim_{\mathbb{F}_p, \mathbb{T}}^* S_2(\Gamma_0(p); \mathbb{F}_p).$$

The number  $\alpha_p \in [0, 1]$  measures “how close” the inequality (10) comes to proving the Hecke-simplicity of  $S_{p+1}(\Gamma(1); \mathbb{Q})$  implied by Maeda’s conjecture.

Note that since  $\dim_{\mathbb{F}_p, \mathbb{T}}^* S_2(\Gamma_0(p); \mathbb{F}_p) \leq \dim_{\mathbb{Q}, \mathbb{T}}^* S_2(\Gamma_0(p); \mathbb{Q})$ , the existence of the Atkin–Lehner involution on  $S_2(\Gamma_0(p); \mathbb{Q})$  implies that  $\limsup_{p \rightarrow \infty} (\alpha_p) \leq \frac{1}{2}$ . Nonetheless, if one could show that  $\{\alpha_p\}_p$  is bounded below by some threshold with high probability, this would constitute considerable progress towards Maeda’s conjecture. If one is willing to speculate that the decompositions of  $S_2(\Gamma_0(p); \mathbb{F}_p)^{\pm}$  into simple  $T_{\ell}$ -modules resemble the cycle decompositions of random permutations, this approach does not seem totally unrealistic.

**Conjecture 5.1** (Imprecise form). *Let  $D_p^{\pm} = \dim_{\mathbb{Q}} S_2(\Gamma_0(p); \mathbb{Q})^{\pm}$  and fix a prime  $\ell$ .*

*The factorization type of the characteristic polynomial of  $T_{\ell}$  acting on  $S_2(\Gamma_0(p); \mathbb{F}_p)$  is distributed like the cycle type of  $\sigma_+ \sqcup \sigma_-$  where  $\sigma_+$  and  $\sigma_-$  are independently chosen random permutations on  $D_p^+$  and  $D_p^-$  elements, respectively.<sup>8</sup>*

<sup>8</sup>More precisely, we believe that  $\mathbb{T}_{\pm, \text{red}}$ , the reduced quotient of the image of  $\mathbb{T}$  in  $\mathrm{End}(S_2(\Gamma_0(p); \mathbb{F}_p)_{\pm})$ , behave like two independent étale  $\mathbb{F}_p$ -algebras distributed according to the random permutation model from [20]. The “longest cycle of  $T_2$ ” statistic studied in this subsection is very unlikely to differ substantially from the “longest cycle of  $\mathbb{T}_{\pm, \text{red}}$ .” Any discrepancy between these two statistics would correspond to the projection of  $T_2$  onto the largest simple factor of  $\mathbb{T}_{\pm, \text{red}}$  (an extension of  $\mathbb{F}_p$  of large degree) landing in a proper subfield.

We have tested Conjecture 5.1 numerically for  $\ell = 2$ . To put the results in context, we first recall a special function which describes the distribution of the longest cycle length in large random permutations.

**Definition 5.2.** The Dickman function  $\rho$ , defined by  $\rho(u) = 1$  on  $u \in (0, 1]$  and by

$$\rho(u) = \frac{1}{u} \int_{u-1}^u \rho(t) dt$$

for  $u > 1$ , captures the statistics of long cycles in random large permutations [12]: the probability that a randomly chosen permutation on  $N$  elements has longest cycle of length  $\leq \frac{N}{u}$  approaches  $\rho(u)$  as  $N \rightarrow \infty$ .

We define random variables  $Y_\ell, Y_\ell^+, Y_\ell^-$  on the set of primes  $\neq \ell$  as follows:

$$Y_\ell(p) = \frac{1}{D_p} \deg_{\mathbb{F}_p}^* \tilde{\Phi}_{p,\ell}(X) \quad \text{and} \quad Y_\ell^\pm(p) = \frac{1}{D_p^\pm} \deg_{\mathbb{F}_p}^* \tilde{\Phi}_{p,\ell}^\pm(X),$$

where  $\tilde{\Phi}_{p,\ell}$  is the characteristic polynomial of  $T_\ell$  on  $S_2(\Gamma_0(p); \mathbb{F}_p)$  and  $\tilde{\Phi}_{p,\ell}^\pm$  is the characteristic polynomial of  $T_\ell$  on  $S_2(\Gamma_0(p); \mathbb{F}_p)^\pm$ . Note that for any  $p$

$$Y_\ell(p) = \max\{Y_\ell^+(p), Y_\ell^-(p)\}.$$

Assuming Conjecture 5.1, we are led to guess that  $Y_\ell^\pm \leq y$  with probability approaching  $\rho(\frac{1}{2y})$ . If  $Y_\ell^+$  and  $Y_\ell^-$  are independent, we would have  $Y_\ell \leq y$  with probability approaching  $\rho(\frac{1}{2y})^2$ .

Using SAGE, we computed  $Y_2(p)$  for all primes  $p \in [100, 10200]$ . The results of this computation are displayed in Figure 4: We have overlaid the CDF of the random variable  $p \mapsto Y_2(p)$  (in light red dots), with the function  $y \mapsto \rho(\frac{1}{2y})^2$  (in blue). The agreement is striking. We conclude with the following conjecture:

**Conjecture 5.3** (Precise form). *For any fixed prime  $\ell$ ,*

$$\lim_{X \rightarrow \infty} \frac{\#\{\text{primes } p \in [X, 2X] : Y_\ell(p) \leq y\}}{\#\{\text{primes } p \in [X, 2X]\}} = \rho\left(\frac{1}{2y}\right)^2.$$

where  $\rho$  is the Dickman function.

For example, Conjecture 5.3 would predict that for a randomly chosen large prime  $p$ ,  $S_{p+1}(\Gamma(1); \mathbb{Q})$  admits a simple Hecke submodule of dimension at least  $\geq \frac{1}{8} \dim_{\mathbb{Q}} S_{p+1}(\Gamma(1); \mathbb{Q})$  with probability  $\geq 0.99997$ .

**Acknowledgements.** We would like to thank Peter Sarnak and Akshay Venkatesh for their encouragement. We are specifically grateful to Akshay Venkatesh for pointing out how to obtain the class number bound in the proof of Corollary 1.7.

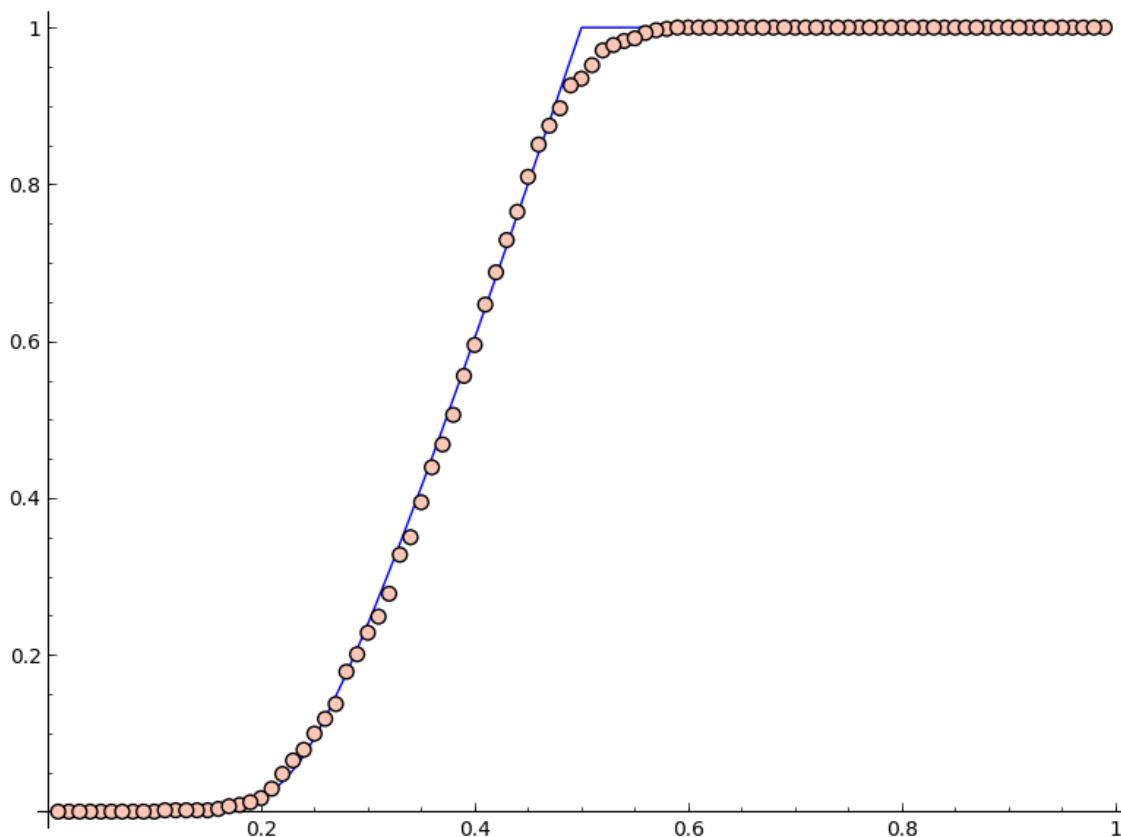


FIGURE 4. The CDF of  $Y_2(p)$  for all primes  $p \in [100, 10200]$  (light red), versus  $u \mapsto \rho\left(\frac{1}{2u}\right)^2$  (blue).

## REFERENCES

- [1] E. Artin. *Collected papers*. Edited by S. Lang and J. Tate. Addison-Wesley, London, 1965.
- [2] A. O. L. Atkin, J. Lehner. *Hecke operators on  $\Gamma_0(m)$* . Math. Ann. **185** (1970) 134–160.
- [3] A. Brumer. *The rank of  $J_0(N)$* . Astérisque **228** (1995) 41–68.
- [4] K. Buzzard. *On the eigenvalues of the Hecke operator  $T_2$* . J. Number Theory **57** (1996) 130–132.
- [5] H. Cohen, H. Lenstra. “Heuristics on class groups of number fields” in *Proceedings of Journées Arithmétiques, Noordwijkerhout 1983*, 33–62. Lecture Notes in Math. **1068**. Springer, Berlin, 1984.
- [6] J. B. Conrey, D. W. Farmer. “Hecke operators and the nonvanishing of L-functions” in *Topics in Number Theory, in Honor of B. Gordon and S. Chowla*, 143–150. Math. Appl. **467**. Kluwer Acad. Publ., Dordrecht, 1999.
- [7] L. Dieulefait, P. Tsaknias. *Possible connection between a generalized Maeda’s conjecture and local types*. arXiv: 1608.05285. Preprint.



- [8] J. S. Ellenberg, A. Venkatesh. *Reflection principles and bounds for class group torsion*. Int. Math. Res. Not. (2007) ID: rnm002.
- [9] M. Emerton. *Optimal quotients of modular Jacobians*. Math. Ann. **327** (2003) 429–458.
- [10] D. W. Farmer, K. James. *The irreducibility of some level 1 Hecke polynomials*. Math. Comp. **71** (2002) 1263–1270.
- [11] A. Ghitza, A. McAndrew. *Experimental evidence for Maeda’s conjecture on modular forms*. Homology, Homotopy and Applications (2012).
- [12] A. Granville. *The anatomy of integers and permutations*. Preprint (2008).
- [13] H. A. Helfgott, A. Venkatesh. *Integral points on elliptic curves and 3-torsion in class groups*. J. Amer. Math. Soc. **19** (2006) 527–550.
- [14] H. Hida, Y. Maeda. *Non-abelian base change for totally real fields*. Pacific J. Math. (1997) Special Issue, 189–217.
- [15] C. Hooley, *On Artin’s conjecture*. J. Reine Angew. Math. **225** (1967) 209–220.
- [16] Iwaniec, Luo, Sarnak. *Low lying zeros of families of L-functions*. Inst. Hautes études Sci. Publ. Math. No. 91 (2000), 55–131 (2001).
- [17] N. Katz. “*p*-adic properties of modular schemes and modular forms” in *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*. Lecture Notes in Math. **350** (1973) 69–190. Springer, Berlin.
- [18] C. Khare. *Modularity of Galois representations and motives with good reduction properties*. J. Ramanujan Math. Soc. **22** (2007) 75–100.
- [19] W. Kohnen, D. Zagier. *Values of L-series of modular forms at the center of the critical strip*. Invent. Math. **64** (1981) 175–198.
- [20] M. Lipnowski. *On Bhargava’s heuristics for  $\mathrm{GL}_2(\mathbb{F}_p)$ -number fields and elliptic curves of bounded conductor*. Preprint.
- [21] C. R. Matthews. *Counting points modulo  $p$  for some finitely generated subgroups of algebraic groups*. Bull. London Math. Soc. **14** (1982) 149–154.
- [22] M. R. Murty, K. Sinha. *Effective equidistribution of eigenvalues of Hecke operators*. J. Number Theory **129** (2009) 681–714.
- [23] E. Royer. *Facteurs  $\mathbb{Q}$ -simples de  $J_0(N)$  de grande dimension et de grand rang*. Bull. Soc. Math. France **128** (2000) 219–248.
- [24] G. J. Schaeffer. *Hecke stability and weight 1 modular forms*. Math Z. **281** (2015) 159–191.
- [25] J.-P. Serre. “Formes modulaires et fonctions zêta  $p$ -adiques” in *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*. Lecture Notes in Math. **350** (1973) 191–268. Springer, Berlin.
- [26] J.-P. Serre. *Répartition asymptotique des valeurs propres de l’opérateur de Hecke  $T_p$* . J. Amer. Math. Soc. **10** (1997) 75–102.
- [27] K. Soundararajan. *The number of imaginary quadratic fields with a given class number*. Hardy-Ramanujan J. **30** (2007) 13–18.
- [28] P. Tsaknias. “A possible generalization of Maeda’s conjecture” in *Computations with modular forms*. Contrib. Math. Comput. Sci. **6** (2014) 317–329. Springer, Heidelberg.

MICHAEL LIPNOWSKI, DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TORONTO.  
*E-mail address*: malipnow@math.utoronto.edu

GEORGE J. SCHAEFFER, DEPARTMENT OF MATHEMATICS, STANFORD UNIVERSITY.  
*E-mail address*: gschaeff.research@gmail.com